UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/645,855	08/22/2003	Bandu Wewalaarachchi	496332000300	8137

25227 7590 08/27/2009

MORRISON & FOERSTER LLP
1650 TYSONS BOULEVARD
SUITE 400
MCLEAN, VA 22102

EXAMINER	
DAVENPORT, MON CHERI S	
ART UNIT	PAPER NUMBER
2416	
MAIL DATE	DELIVERY MODE
08/27/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/645,855	WEWALAARACHCHI ET AL.	
	Examiner	Art Unit	
	MON CHERI S. DAVENPORT	2416	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12 May 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1 and 3-11* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1 and 3-11* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

2. **Claims 1-4** rejected under 35 U.S.C. 102(b) as being anticipated by Wootton et al. (US Patent 6,128,298).

Regarding **claim 1** Wootton et al. discloses a system for supporting a website comprising:

an IP device located on a public network, having a public IP address and known port number(see figure 1, public network with node(devices) section 20 with IP address, see col. 4, lines 64-67, public devices have IP address , see also col. 5, lines 37-50, IP address and port number of public devices) ;

a second device located outside the public network, the second device not including a listening socket(see figure 1, section private network , nodes section 18 nodes(devices) outside of the public network, see col. 4, lines 60-64, see col. 5, lines 30-34, the private nodes initiate the communication);

wherein a connection exists between the second device and the IP device, which connection is initiated by the second device; and the IP device cannot initiate a connection with the second device due to the second device not having a listening socket (see col. 5, lines 16-34, connection or access is obtained from the private nodes to the public network, the private

devices are only accessible through the IP filter, all communication by private node are initiated by the private nodes).

Regarding **Claim 3** Wootton et al. discloses everything as applied above (*see claim 1*).

wherein the second device is located on a private IP network with a private IP address(see col. 4, lines 60-64, the private devices have private IP addresses).

Regarding **Claim 4** Wootton et al. discloses everything as applied above (*see claim 3*).

wherein the communication protocol between the first device and the second device is TCP/IP or application level protocol based on TCP/IP(see col. 5, lines 30-36, the communication between the networks, are TCP/IP).

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. **Claims 5-11** rejected under 35 U.S.C. 103(a) as being unpatentable over Wootton et al in view of Andersson et al. (US Patent 6, 931,016).

Regarding **Claim 5** Wootton et al. discloses everything as applied above (*see claim 1*).

Wootton et al. fails to specifically point out wherein the communication between the first device and the second device is encrypted as claimed.

However Andersson et al. teaches wherein the communication between the first device and the second device is encrypted (see col. 4, lines 17-30, the VPN connection uses secured encryption data).

Therefore it would have been obvious to one with ordinary skill in the art at the time the invention was made to combine Wootton et al.'s invention with Andersson et al. invention because Andersson et al. invention provides a method of managing a virtual private network having a set of network devices maintains a network device memory set for storing a set of network device identifiers that identifies each of the set of network devices (see Andersson et al., col. 1, lines 44-48).

Regarding **Claim 6** Wootton et al. discloses everything as applied above (*see claim 1*).

Wootton et al. fails to specifically point out wherein the second device comprises a memory storing information for publication or private source data as claimed.

However Andersson et al. teaches wherein the second device comprises a memory storing information for publication or private source data (see col. 1 lines 45-49, the virtual private network, have memory sets for storing network device identifiers (private source data)).

Therefore it would have been obvious to one with ordinary skill in the art at the time the invention was made to combine Wootton et al.'s invention with Andersson et al. invention because Andersson et al. invention provides a method of managing a virtual private network having a set of network devices maintains a network device memory set for storing a set of network device identifiers that identifies each of the set of network devices (see Andersson et al., col. 1, lines 44-48).

Regarding **Claim 7** Wootton et al. discloses everything as applied above (*see claim 1*).

Wootton et al. fails to specifically point out further comprising a third device connected to the second device through a private network, the third device comprising a memory storing information for publication or private source data as claimed.

Andersson et al. teaches further comprising a third device connected to the second device through a private network, the third device comprising a memory storing information for publication or private source data(see col. 1 lines 45-49, the virtual private network, have memory sets(which reads on third or more than one) for storing network device identifiers (private source data)).

Therefore it would have been obvious to one with ordinary skill in the art at the time the invention was made to combine Wootton et al.'s invention with Andersson et al. invention because Andersson et al. invention provides a method of managing a virtual private network having a set of network devices maintains a network device memory set for storing a set of network device identifiers that identifies each of the set of network devices (see Andersson et al., col. 1, lines 44-48).

Regarding **claim 8** Wootton et al. discloses a system for supporting a website comprising an IP device located on a public network, the IP devicehaving a public IP address and known port number (see figure 1, public network with node (devices) section 20 with IP address, see col. 4, lines 64-67, public devices have IP address, see also col. 5, lines 37-50, IP address and port number of public devices);

a second device located on a private network having a responder function with a private IP address and port number, the second device not including a listening socket;(see col. 5, lines 16-34, connection or access is obtained from the private nodes to the public network, IP filter reads on responder function, the private nodes initiate communication);

wherein a single connection exists between the second device and the first device, which connection is initiated by the second device and wherein the first device cannot initiate a connection with the second device by virtue of the second devices private and dynamic IP address(see col. 5, lines 16-20, the private devices are only accessible through the IP filter).

Wootton et al fails to specifically point a third device having a memory, storing information for publication or private source data, located on the private network in communication with second device as claimed.

However Andersson et al. teaches a third device having a memory, storing information for publication or private source data, located on the private network in communication with second device(see col. 1 lines 45-49, the virtual private network, have memory sets(which reads on third or more than one) for storing network device identifiers (private source data)).

Therefore it would have been obvious to one with ordinary skill in the art at the time the invention was made to combine Wootton et al.'s invention with Andersson et al. invention because Andersson et al. invention provides a method of managing a virtual private network having a set of network devices maintains a network device memory set for storing a set of network device identifiers that identifies each of the set of network devices (see Andersson et al., col. 1, lines 44-48).

5. **Claims 9, 10 and 11** rejected under 35 U.S.C. 103(a) as being unpatentable over Wootton et al. in view of Foulkes et al. (WO 02/30082 A2).

Regarding **Claim 9** Wootton et al. discloses a method for increasing security for sensitive information or source data contained in a memory which is used to respond to inquiries directed to a website by safeguarding a responder function, comprising:

providing on a public network an IP device having a public IP address and known port number, (see Wootton et al., figure 1, public network with node (devices) section 20 with IP address, see col. 4, lines 64-67, public devices have IP address, see also col. 5, lines 37-50, IP address and port number of public devices);

the listening application receiving a request from a remote application and sending incoming requests only to the registered responder application (see Wooton et al. , see col. 5, lines 1-40, the IP filter acts as gateway through which data packets are exchanged between private network and public network, the registered responder(IP filter) , Listening application(public)and remote application (private))

Foulkes et al. teaches the IP device having an application that corresponds to a listening function of a website (see page 9, lines 12-22, security server).

providing an application corresponding to a responder function of a website wherein the responder application is isolated from the IP device(see Foulkes et al., page 11, lines 4-12, figure 4, shows a IP device with a responder function, responding to request);

the responder application registering with the listening application and subscribing to receive incoming requests by initiating a communication channel to the listening application as a communication client (see Foulkes et al., page 9, lines 12-22, the client IP application generates

IP request through the web browser, which includes a flag to identify the security server (listening function) of request, connection is established);

the listening application receiving a request from a remote application and sending incoming requests only to the registered responder application (see page 11, lines 3-6, the security server receives a validation request form the secure server , the validation request contain profile information , which is used to determine whether the user is valid or not, which allows receiving request only to registered(valid) responder application);

processing the incoming requests by the responder application(see Foulkes et al., page 9, lines 12-22, the web browser generates the IP request passed to the IP Application (responder application); and

returning results to the remote application via listening application(see Foulkes et al, page 9, lines 12-22, the security server responds with an IP request for the profile, which is received by the IP application).

Therefore it would have been obvious to one with ordinary skill in the art at the time the invention was made to combine Wootton et al.'s invention with Foulkes et al. invention because Foulkes et al. invention provides a system for controlling access by clients to servers over an Internet protocol network to which authorized persons can gain access (see Foulkes et al. page 1, lines 3-5).

Regarding **Claim 10** Wootton et al. discloses a method for increasing security for sensitive information or source data contained in a memory which is used to respond to inquiries directed to a website by allowing them to be placed in a private network along with a responder function comprising:

providing on a public network an IP device having a public IP address and known port number, (see Wootton et al., figure 1, public network with node (devices) section 20 with IP address, see col. 4, lines 64-67, public devices have IP address, see also col. 5, lines 37-50, IP address and port number of public devices);

providing on a private network a second IP device having a private IP address, (see Wootton et al., col. 5, lines 16-20, connection or access is obtained from the private nodes to the public network);

processing the incoming requests by the responder application by optionally accessing the source data(see Wootton et al. , col. 5, lines 1-40, the request is initiated by the private node, and send communication via the IP filter,)

returning results to the remote application via the listening application(see Wooton et al. col. 5, lines 1-40, the IP filer acts a gateway through which the data packets exchange between the private network)

Foulkes et al. teaches the IP device having an application that corresponds to a listening function of a website (see page 9, lines 12-22, security server);

the second IP device having an application corresponding to a responder function of a website(see Foulkes et al., page 11, lines 4-12, figure 4, shows a IP device with a responder function, responding to request);

the responder application initiating an outgoing TCP connection to the listening application as a communication client and registering to receive incoming requests(see Foulkes et al., page 9, lines 12-22, the client IP application generates IP request through the web browser,

which includes a flag to identify the security server (listening function) of request, connection is established);

the listening application receiving a request from a remote application and sending incoming requests to the responder application (see page 11, lines 3-6, the security server receives a validation request from the secure server, the validation request contain profile information, which is used to determine whether the user is valid or not, which allows receiving request only to registered (valid) responder application);

processing the incoming requests by the responder application by optionally accessing the source data(see page 11, lines 22-28, the IP session is open and the data carried by the IP packet is read and authenticated, target server is able to carry out further levels of authentication (using HTTP, CGI script) reads on optionally accessing the source data);

returning results to the remote application via the listening application(see Foulkes et al, page 9, lines 12-22, the security server responds with an IP request for the profile, which is received by the IP application).

Therefore it would have been obvious to one with ordinary skill in the art at the time the invention was made to combine Wootton et al.'s invention with Foulkes et al. invention because Foulkes et al. invention provides a system for controlling access by clients to servers over an Internet protocol network to which authorized persons can gain access (see Foulkes et al. page 1, lines 3-5).

Regarding **claim 11** Wootton et al. discloses a method for increasing security for sensitive information which is used to respond to inquiries directed to a website, comprising:

providing on a private network an IP device having a dynamic IP address and port number(see Wootton et al., col. 5, lines 16-20, connection or access is obtained from the private nodes to the public network),

providing on a public network a second IP device having a public IP address and known port number(see Wootton et al. , figure 1, public network with node (devices) section 20 with IP address, see col. 4, lines 64-67, public devices have IP address, see also col. 5, lines 37-50, IP address and port number of public devices),

causing the responder application in the first device to establish a connection with the listening application in the second device, the communication including the IP address for the first device and a port number for the responder application (see Wootton et al., col. 5, lines 16-20, connection or access is obtained from the private nodes to the public network, IP filter reads on responder application function);

receiving communications at the second IP device from other IP devices located on the public network or from devices located on private networks in communication with the public network (see Wootton et al. , col. 5, lines 1-4, communication is established via the IP filter between the private and public network);

providing on a private network a second IP device having a private IP address, (see Wootton et al., col. 5, lines 16-20, connection or access is obtained from the private nodes to the public network);

processing the incoming requests by the responder application by optionally accessing the source data(see Wootton et al. , col. 5, lines 1-40, the request is initiated by the private node, and send communication via the IP filter,)

returning results to the remote application via the listening application(see Wooton et al. col. 5, lines 1-40, the IP filer acts a gateway through which the data packets exchange between the private network)

Foulkes et al. teaches the IP device having an application corresponding to the responder function of a website(see Foulkes et al., page 11, lines 4-12, figure 4, shows a IP device with a responder function, responding to request);

the second IP device having an application that corresponds to the listening function of a website, the IP device not including a listening socket(see Foulkes et al., page 8, lines 14-16, the second device (secure server, waits to receive profile, which reads on listening function);

transmitting requests for application relating to the inquiries from the listening application to the responding application over the connection established by the responding the application(see Foulkes et al., page 9, lines 12-22, the client IP application generates IP request through the web browser, which includes a flag to identify the security server(listening function) of request, connection is established) ;

processing the request for information by the responder application(see Foulkes et al., page 9, lines 12-22, the web browser generates the IP request passed to the IP Application (responder application)

providing a response from the responder application to the listening application over the connection established by the responder application(see Foulkes et al;, page 9, lines 12-22, the IP application responds with an acknowledgement that carries a profile to the security server over the established connection); and

transmitting from the listening application to the other IP device information relating to the request(see Foulkes et al, page 9, lines 12-22, the security server responds with an IP request for the profile, which is received by the IP application).

Therefore it would have been obvious to one with ordinary skill in the art at the time the invention was made to combine Wootton et al.'s invention with Foulkes et al. invention because Foulkes et al. invention provides a system for controlling access by clients to servers over an Internet protocol network to which authorized persons can gain access (see Foulkes et al. page 1, lines 3-5).

Response to Arguments

6. Applicant's arguments filed 5/12/2009 have been fully considered but they are not persuasive.

In the remarks on pgs. 6-7 of the amendment, the applicant contends that Wooton does not teach or suggest "a second device located outside the public network, the second device not including a listening socket; wherein… the IP device cannot initiate a connection with the second device due to the second device not having a listening socket"

Examiner respectfully disagrees Wooten teaches the private nodes initiate the communication, therefore no listening socket, nodes can not be reached, they most initiate.

In the remarks on pg. 7 of the amendment, the applicant contends that Wooton and Foulkes does not teach or suggest "the listening application receiving a request from a remote application and sending incoming request only to the registered responder application"

Examiner respectfully disagrees Wooten teaches the IP filter acts as gateway through which data packets are exchanged between private network and public network, the (registered responder) reads on IP filter, (listening application)reads on public and (remote application)reads on private.

In the remarks on pg. 8 of the amendment, the applicant contends that Wooton and Foulkes do not teach or suggest "processing the incoming request by the responder application; and returning results to the remote application via the listening application"

Examiner respectfully disagrees Wooten teaches the request is initiated by the private node, and send communication via the IP filter, the IP filer acts a gateway through which the data packets exchange between the private network.

Conclusion

7. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period

will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MON CHERI S. DAVENPORT whose telephone number is (571)270-1803. The examiner can normally be reached on Monday - Friday 8:00 a.m. - 5:00 p.m. EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Seema Rao can be reached on 571-272-3174. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Seema S. Rao/
Supervisory Patent Examiner, Art Unit 2416

/Mon Cheri S Davenport/

Examiner, Art Unit 2416
August 20, 2009